Deloitte.

Banking spotlight

Global risk management survey, 11th edition

Reimagining risk management to mitigate looming economic threats and nonfinancial risks

Executive summary

As they battle nontraditional competitors in a rapidly shifting marketplace, banking institutions are facing a series of impending economic perils and nonfinancial risks. Economic storm clouds remain on the horizon in the form of tensions over tariffs between the United States, China, the European Union (EU), and other jurisdictions. Global growth has been slowed by weak economic performance in Europe, coupled with a more slowly growing Chinese economy saddled with increasing debt levels. There are also concerns that the world economy may be ready for another in a series of periodic crises that have hit markets and reduced growth periodically over the last several decades.

Although the speed of regulatory change has slowed, a number of important regulatory requirements remain to be finalized, while the full implications of those that have been recently implemented are still being assessed. Individual jurisdictions have not decided how they will implement, and whether they will vary, the final Basel III revisions to the capital framework. The European Union's General Data Protection Regulation (GDPR), which took effect in May 2018 and applies to all firms that collect information from EU citizens, has placed new requirements on how banks collect and use consumer data and will require significant changes to data governance and IT systems.

In the midst of these uncertainties, some banks are preparing to shift from a traditional closed model to a more customer-centric and flexible "open banking" model, in which data is shared among different financial providers with the authorization of the customer. Fintech competitors, which leverage technology capabilities to introduce innovative new products and directly target customers, are not confined to startups but also include major technology and e-commerce companies that bring preexisting customers and strong brands.

Banks will need to rethink their risk management approaches to meet these challenges, from increasing their focus on nonfinancial risks to leveraging the latest AI technologies. Deloitte's *Global risk management survey, 11th edition,* the latest edition in this ongoing survey series, includes responses from 57 banking institutions on their risk management practices and challenges. Five key takeaways emerged for banks:

- Growing threats from cybersecurity risk
- Managing an array of nonfinancial risks
- Unleashing the power of digital risk management
- Strengthening risk data and IT systems
- Reassessing the three lines of defense model

Growing threats from cybersecurity risk

A variety of cyberattacks have led to an increased focus on managing cybersecurity risk by regulators and banks. The Cobalt hacking group has been associated with cyberattacks against at least 100 banks around the world since 2016, stealing approximately one billion euros.[1] In July 2017, an Italian bank had confidential data from 400,000 customer accounts stolen by hackers.[2] The US Treasury Department has named cyberattacks one of the top risks facing the US financial sector.[3]

Cyberattacks are increasing in sophistication and can inflict significant financial and reputational damage on banks through a wide variety of means such as theft of client data or other confidential information, installing ransomware, initiating unauthorized payments, conducting commercial espionage, and disrupting online systems. Regulatory authorities around the world have undertaken initiatives to strengthen their supervision of cybersecurity including in the United States, the United Kingdom, the European Union, Hong Kong, and Singapore.

Sixty-six percent of banks named *cybersecurity* as one of three risks that would increase the most in importance for their institution over the next two years, far more than for any other risk, with 41 percent ranking it as No. 1 . Yet, only 48 percent of banking respondents felt their institutions were extremely or very effective in managing this risk. The cybersecurity issues that banks most often said were extremely or very challenging were *hiring or acquiring cybersecurity talent* (61 percent) and *staying ahead of changing business needs* (e.g., social mobile, analytics, cloud) (59 percent). See figure 1.

Figure 1
In your opinion, how challenging is each of the following for your organization in managing cybersecurity risk?
Base = Respondents at banks

Given the increase in cyberattacks, there has been a fierce competition for professionals with cybersecurity skills. Banks will need to supplement human expertise with technology tools such as predictive analytics that can identify potential threats before they occur. In addition, many banks will need to reexamine their sourcing of capabilities from third parties, revisit their strategies, and assess their level of industry collaboration.

Managing an array of nonfinancial risks

In addition to cybersecurity, additional nonfinancial risks are also assuming greater importance. A series of well-publicized instances of inappropriate conduct at major banks has increased the attention paid to managing conduct and culture risk, leading to regulatory initiatives in Australia, the United States, the United Kingdom, Europe, and Hong Kong, among other jurisdictions.[4]

Banks face third-party risk from the potential that one of its service providers fails to perform or engages in unethical conduct, which could result in regulatory noncompliance and reputational damage.

Complying with anti-money laundering requirements is another challenge. In 2018, there were prominent instances of alleged money laundering in Malta and Denmark, leading the European Banking Authority to launch a review into how all EU member states are applying rules in this area.[5]

"Nonfinancial risks are growing in size and importance. The focus has moved beyond traditional operational risks to risks like cyber, conduct and culture, and third-party risk management. Dealing with the challenges posed by these risks requires additional resources."

— **Senior risk executive**
Large diversified financial services company

While more than 90 percent of banking respondents considered their institutions to be extremely or very effective in managing financial risks, such as market, credit, and liquidity risk, less than half said the same about nonfinancial risks: *third-party* (45 percent), *conduct and culture* (44 percent), *systemic* (40 percent), and *geopolitical* (36 percent). Deploying advanced analytics and AI technologies will be an important element of an effective strategy to manage these risks.

Unleashing the power of digital risk management

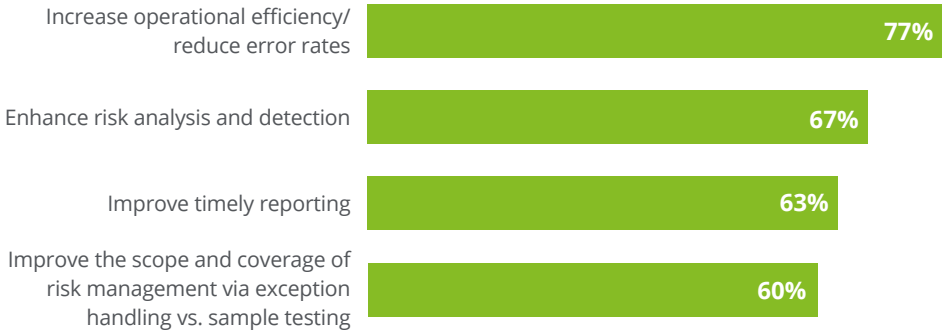
Banks will need to reengineer risk management by employing the latest technologies and digital tools, such as big data, cloud computing, robotics and process automation, cognitive analytics, and natural language processing. These tools can significantly reduce expenses by automating routine, manual tasks. They can also improve the effectiveness and foresight of risk management by identifying emerging threats, providing insight into their causal factors, and allowing institutions to take preventive action before risk events occur. They also make it possible to automatically review 100 percent of a set of transactions, rather than rely on human review of only a sample.

Banks see the potential for substantial benefits from emerging technologies, with respondents most often expecting very large or large benefits in *increase operational efficiency/reduce error rates* (77 percent), *enhance risk analysis and detection* (67 percent), and *improve timely reporting* (63 percent) (see figure 2). Roughly half the respondents expected new technologies to provide this level of benefit to *improve the scope and coverage of risk management via exception handling vs. sample testing* (60 percent) and *reduce costs* (56 percent).

"We are using a variety of new technologies. For example, we are using automation for processing data and reporting, and are building tools for automatically monitoring compliance and BSA/AML, as well as our reputation in the marketplace."

— **Chief risk officer**
Major multinational bank

Figure 2
How much potential benefit do you believe that your organization could gain in each of the following risk management areas from the application of emerging technologies?
Base = Respondents at banking institutions
Percentage responding "extremely/very large benefit"



Strengthening risk data and IT systems

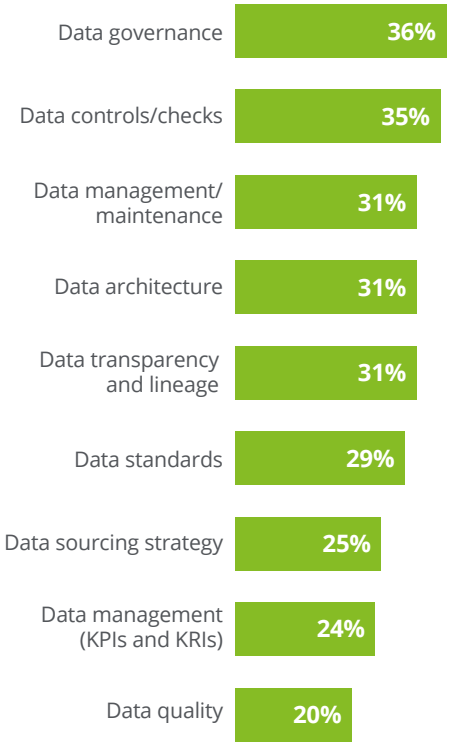
Employing advanced technologies will depend on having access to relevant data and the necessary digital capabilities in the risk management IT infrastructure, both of which are challenging for many banks. Providing quality data from the source through many systems and processes to the ultimate users has been a long-standing difficulty for many institutions.

Regulators are requiring banks to improve their risk data. The Basel Committee released principles for effective risk data aggregation and risk reporting (BCBS 239) in 2013, but the group's June 2018 progress report concluded that banks had found it "challenging to comply with the Principles."[6] The United States, Australia, and India are among the countries that increased their attention to supervision of risk data management.

When asked about the risk management priorities for their institutions over the next two years, banking respondents most often cited issues related to data and IT systems were an extremely or very high priority: *enhancing the quality, availability, and timeliness of risk data* (86 percent) and *enhancing risk information systems and technology infrastructure* (75 percent). This is consistent with the fact that few banking respondents believed their institutions are extremely or very effective in such areas as *data quality* (20 percent), *data management/ maintenance* (31 percent), *data sourcing strategy* (25 percent), and *data standards* (29 percent) (see figure 3).

Many banks will require significant work to implement an integrated data architecture and an effective data controls framework. Rather than leaving data to be housed in business units, more banks are moving to viewing data as enterprise assets managed by the C-suite, with some creating a chief data officer (CDO) position.

Figure 3
How effective do you think your organization is in each of the following aspects of risk data strategy and infrastructure?
Base = Respondents at banking institutions
Percentage responding "extremely/ very effective"



Reassessing the three lines of defense model

Virtually all banks (96 percent) reported employing the three lines of defense risk governance model. While the concept behind the model is sound, the issues most often cited as significant challenges in employing the model related to clarifying the risk management responsibilities of line 1 (business units): *defining the roles and responsibilities between line 1 (business) and line 2 (risk management)* (51 percent), *getting buy-in from line 1 (business)* (45 percent), and *having sufficient skilled personnel in line 1* (42 percent), and *executing line 1 responsibilities* (36 percent) (see figure 4).

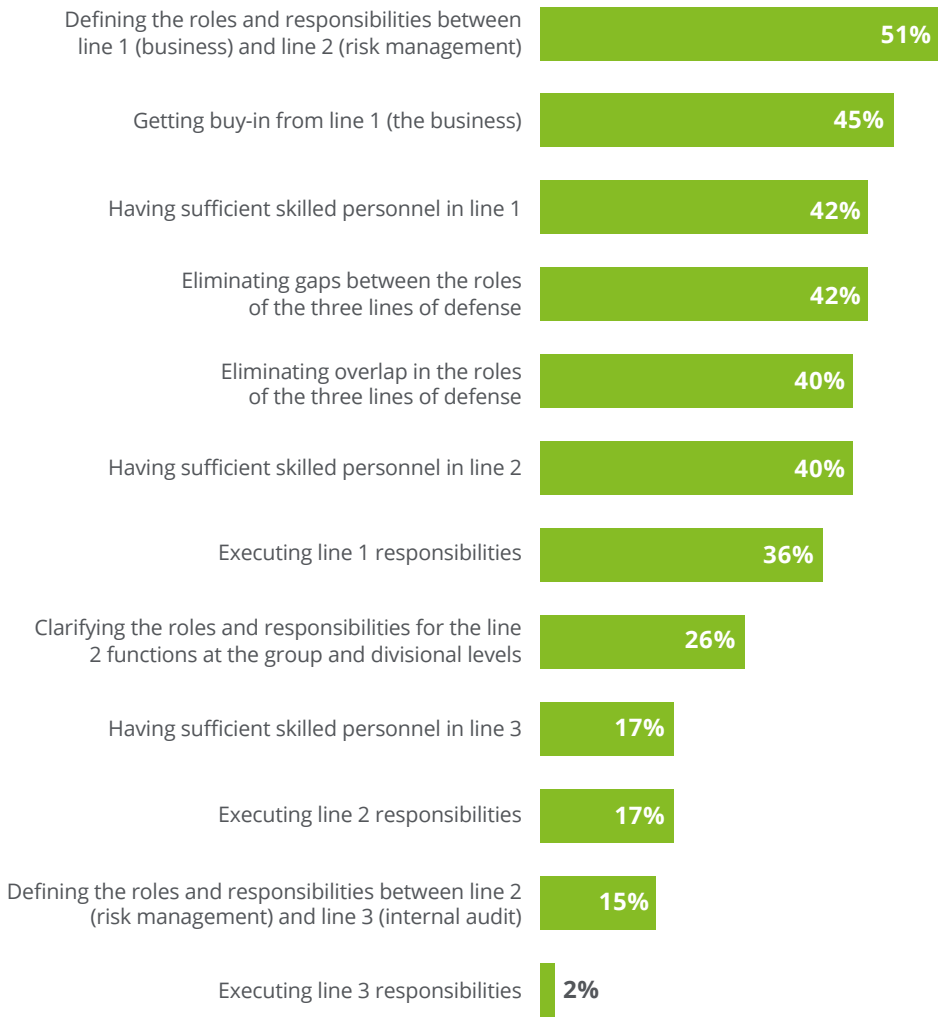
Although the three lines of defense model is based on the premise that the business units in line 1 are responsible for managing the risks they assume, this is not easy to achieve. Risk management is still considered to be outside the core mission of business units, which are rewarded on their ability to generate revenues and profits. Even when business units buy in to their risk management role, they may lack sufficient professionals with the relevant skills. It is often difficult to hire skilled professionals who combine risk management expertise with experience in the specific business.

As a result, 51 percent of banks said they had revised or are planning to reassess their three lines of defense models. In many cases, banking regulators are also encouraging banks to enhance their risk governance models including in their nonbanking operations.

"Some of our biggest challenges with the first line of defense in managing risk are making sure that they take responsibility for ownership of their risks and training them so that they are knowledgeable about the risk issues."

— **Chief risk officer**
Major multinational bank

Figure 4
What are the most significant challenges your organization faces in maintaining a "three lines of defense" risk governance model?
Base = Respondents at banking institutions



Conclusion

Banks are adopting new business models and competing with nontraditional competitors against a backdrop of economic threats and burgeoning nonfinancial risks. Successfully meeting these demands will require new approaches for risk management—intensifying management of nonfinancial risks such as cybersecurity, conduct, fraud, data integrity, and third-party risk; leveraging the capabilities of digital technologies; enhancing risk data governance and IT systems; and reassessing the three lines of defense governance model. Banks will need to fundamentally transform their risk management approaches if they are to prosper in this rapidly evolving competitive environment.

Global risk management survey, 11th edition

Global risk management survey, 11th edition is the latest edition in Deloitte's ongoing survey series that assesses the state of risk management in the financial services industry and the challenges it faces. The 2018 survey findings are based on the responses of 94 financial institutions around the world, including 57 banking institutions. These banks represented a range of sizes as measured by their consolidated assets: 17 percent with less than US$10 billion, 37 percent with US$10 billion to less than US$100 billion, and 46 percent with US$100 billion or more. To view the full report, please visit https://www.deloitte.com/insights/globalrisksurvey.

Endnotes

1 "Mastermind Behind Eur 1 Billion Cyber Bank Robbery Arrested in Spain," Europol, Press Release, March 26, 2018, https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain.

2 Sofia Petkar, "Italy's largest bank HACKED in major security breach as data from 400,000 accounts stolen," *Express*, July 27, 2017, https://www.express.co.uk/finance/city/833440/italy-unicredit-bank-hacked-cyberattack-italian-banking-major-security-breach.

3 Office of Financial Research, US Department of the Treasury, *2017 Annual Report to Congress*, December 5, 2017, https://www.financialresearch.gov/annual-reports/2017-annual-report/.

4 For a discussion of these regulatory developments, see Deloitte, *Financial services regulatory outlook 2018: Facing the future: An evolving landscape*, Deloitte Centre for Regulatory Strategy, Asia Pacific, 2017.

5 "EU watchdog criticizes Malta for anti-money laundering shortcomings," Reuters, July 11, 2018, https://www.reuters.com/article/us-malta-banks-eu/eu-watchdog-criticizes-malta-for-anti-money-laundering-shortcomings-idUSKBN1K12NS; Huw Jones, "EU bank watchdog examining Danish handling of Danske," Reuters, October 8, 2018, https://www.reuters.com/article/us-eu-danske-regulator/eu-bank-watchdog-examines-danske-banks-supervisor-idUSKCN1MI1J7.

6 Bank for International Settlements (BIS), *Progress in adopting the Principles for effective risk data aggregation and risk reporting*, Basel Committee on Banking Supervision, June 2018, https://www.bis.org/bcbs/publ/d443.pdf.

Contacts

Global financial services industry leadership

Bob Contri
Global leader | Financial Services Industry
Deloitte Global
+1 212 436 2043
bcontri@deloitte.com

Anna Celner
Global leader | Banking & Capital Markets
Deloitte Global
+41 58 279 6850
acelner@deloitte.ch

J.H. Caldwell
Global Financial Services leader | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 704 227 1444
jacaldwell@deloitte.com

Survey editor

Edward T. Hida II, CFA
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 4854
ehida@deloitte.com

Acknowledgments

This report is the result of a team effort that included contributions by financial services practitioners from member firms of Deloitte Touche Tohmatsu Limited around the world. Special thanks are given to Bayer Consulting for administering the survey and assisting with the final document.

Subject matter advisor

Bruno Melo, Toronto, Ontario, Canada
brmelo@deloitte.ca

Deloitte.